1. TEORÍA DE CONJUNTOS.

Conjunto: colección <u>desordenada</u>. }elementos{
Lista: colección <u>ordenada</u>. [elementos]

$V = \{1,2,3\}$
$\omega = \{1,2,3,2\}$ $\quad V = \omega$

$card(V) = 3$; $card(\omega) = 3$

$N = \{2,3\}$

$N \subset V$; $V \subseteq \omega$; $N \subsetneq V$; $\{\phi\} \subset V$; $\phi \in V$; $N \subset \mathbb{N}$

- Diagramas de Venn
- Operaciones: asociativa, distributiva, conmutativa, identidad, idempotencia, complemento, <u>de Morgan</u>

$A \cup B$; $A \cap B$; $A \pm B$

$\sqcup \rightarrow$ Universo

$\bar{A} \leftrightarrow A$

<u>de Morgan</u> $\quad \overline{A \cup B} = \bar{A} \cap \bar{B}$; $\overline{A \cap B} = \bar{A} \cup \bar{B}$

<u>FUNCIONES</u>

RELACIONES: Relacionan <u>todos</u> los conjuntos de A con alguno de B
APLICACIONES: Relaciones que relacionan <u>todos</u> los conjuntos de a con un único conjunto de B.
INYECTIVA: Función que es aplicación y cuyas imágenes son todas únicas.
SOBREYECTIVA: Si todo elemento de B es imagen de alguno de A.
BIYECTIVA: Inyectiva y sobreyectiva.

- COMPOSICIÓN DE FUNCIONES: No conmutativo, asociativo

  Requiere: $Dom(f) = Rg(g)$

  $g \circ f(a) = g[f(a)]$

$\lfloor \rfloor$ FLOOR $\lceil \rceil$ CEIL

- RELACIONES

  - Reflexiva: unos en la diagonal
  - Simétrica: coincidir con la traspuesta.
  - Antisimétrica: nada coincide con la traspuesta.
  - Transitiva: cuando dos relaciones cumplen $(a,b); (b,c) \Rightarrow (a,c)$

Reflexiva + simétrica + transitiva: de EQUIVALENCIA
Reflexiva + antisimétrica + transitiva: de ORDEN { TOTAL: Debe ser divisibles entre sí / PARCIAL

- Diagramas de orden: HASSE

- ORDENACIÓN TOPOLÓGICA.

  - Elementos minimales.

2. LÓGICA DE PROPOSICIONES

CONJUNCIÓN	$p \wedge q$	NEGACIÓN	$\neg p$
DISYUNCIÓN	$p \vee q$	IMPLICACIÓN	$p \to q$
DISYONCIÓN EXCLUSIVA	$p \oplus q$	DOBLE IMPLICACIÓN	$p \leftrightarrow q$

- TAUTOLOGÍA
- CONTRADICCIÓN
- CONTINGENCIA

EQUIVALENCIA LÓGICA : Si $p \leftrightarrow q$ es <u>tautología</u>

Idempotencia, conmutativa, asociativa, distributiva, identidad, absorción, DeMorgan

<u>Argumento</u> : hipótesis $\longrightarrow$ teorema

REGLAS DE INFERENCIA:

$p \wedge (p \to q) \Rightarrow q$

$(p \to q) \wedge (q \to r) \Rightarrow p \to r$

$(p \to q) \wedge \neg q \Rightarrow \neg p$

$(p \vee q) \wedge \neg q \Rightarrow p$

$\wedge \neg p \Rightarrow q$

$\neg p \to F \Rightarrow p$

- DUAL DE UNA PROPOSICIÓN:

$Dual(p) \Leftrightarrow Dual(q)$

si

$p \Leftrightarrow q$

$Dual(p) = ch(\wedge\neg\vee, \vee\_\wedge)$

- Proposición abierta: con <u>variables</u>, no puede ser evaluada tal cual.

3. MÉTODOS DE DEMOSTRACIÓN

3.1 MÉTODO DIRECTO

Ejemplo:

~~$\forall x^3$ impar $\Rightarrow x$ impar~~

$q \longrightarrow p \iff \neg p \longrightarrow \neg q$

$$\frac{p \qquad p \to q}{q}$$

3.2 MÉTODO INDIRECTO

Ejemplo:

$\forall x^3$ impar $\Rightarrow x$ impar

x par $\rightarrow$ x^3 par

$n = 2a$

$n^3 = (2a)^3 = 8 \cdot a^3 = 2 \cdot 4a^3$

$\neg q \longrightarrow \neg p$

3.3 CONTRADICCIÓN

$\sqrt{2}$ es irracional

DEMOSTRAMOS: $\sqrt{2}$ es irracional

$$\sqrt{2} = \frac{a}{b} \; ; \quad 2 = \frac{a^2}{b^2} \Rightarrow a^2 = 2b^2$$

$\downarrow$

factores en común $\longrightarrow$ irracional

3.4 INDUCCIÓN

Ejemplo:

$x^n + y^n = z^n$ no tiene solución entera para $n > 2$

- Se "demuestra" para $n = n_1$ (supone cierto)
- Se demuestra para $n = n_{1+1}$

⇓

Cierto $\forall n$

$\forall n$, $7^n + 5$ es divisible por 3.

$P(1) = 7^1 + 5 = 3 \cdot 4$ CIERTO

$P(k+1) = 7^{k+1} + 5 = 3 \cdot b$

$7^k \cdot 7 + 5 = 3b$

$7^k (6+1) + 5 = 3b$

$\underbrace{7^k \cdot 6}_{\times 3} + \underbrace{7^k + 5}_{\times 3} = 0$ CIERTO

3.4.1 INDUCCIÓN FUERTE

Ejemplo: Un jugador gana cuando el otro quita la última cerilla de uno de los montones.

$1 \leq (k+1-j) \leq k$ $\quad j \quad j \leq k$

4. ÁLGEBRA DE BOOL

→ Cosas anteriores: ejemplos de álgebras de bool.

→ Propiedades: conmutativa, asociativa, idempotencia, neutro

· Función booleana $B^n \longrightarrow B$

TERMÍNIMOS (SOP): $X_1 X_2 \overline{X_3} + \overline{X_2} X_0$

TERMÁXIMOS (POS): $(X_1 + X_2 + \overline{X_3}) \cdot (X_1 + \overline{X_2})$

- SIMPLIFICAR (algebraicamente, Karnaugh, Quine-Mc.Cluskey)
- CIRCUITOS
-

5. ARITMÉTICA ENTERA Y MODULAR.

a divide a b si $\exists\, c / b = ac$

$b = \dot{a}$

→ Propiedades:

- Si a divide a b y a divide c → a divide $(b+c)$.
- Si a divide a b, divide a cualquier múltiplo.
- Si a divide a b, y b divide a c → a divide a c.

· Números primos: divisibles entre el mismo número y 1 tan sólo

EL 1 NO ES PRIMO.

T^ma fundamental de la aritmética:

Todo número $\in \mathbb{Z}^{+}$ se puede escribir como producto de números primos.

- Todo nº primo no es divisible por un número menor que $\sqrt{n^{o}}$

- ECUACIÓN LINEAL DIOFÁNTICA.

→ Solución si MCD(a,b) divide a c. Soluciones infinitas.

$$\underline{a}x + \underline{b}y = \underline{c}$$

- INVERSO:

Ej: $\mathbb{Z}/_{212} \Rightarrow \{1, 5, 7, 11\}$

phi (numero) = (factor$_1$ − 1) * (factor$_2$ − 1) ... * m (factor$_n$ − 1)

$\mathbb{Z}/_{9}$ → unidades = {1,2,4,5,7,8} PF. no tienen que ver con el número.

→ APLICACIONES:

CRITERIOS DE DIVISIBILIDAD:

$$\text{Si } a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + 10_1\ 10 + a_0$$

→ a es Divisible por...

→ 2 si a_0 es par

→ 4 si $a_1 a_0$ es divisible por cuatro

→ 8 si $a_2 a_1 a_0$ es divisible por ocho

→ (3||9) si $a_n + a_{n-1} \ldots + a_0$ es múltiplo de (3||9)

→ 5 si a_0 es divisible por cinco

→ 11 si $(-1)^n \cdot a_n + a_{n-1} + \ldots + a_2 - a_1 + a_0$ es divisible por 11.

USO DE CONGRUENCIAS

→ Números pseudoaleatorios:

x_0 → valor inicial
m → valor máximo

$$\text{aleatorio}(x_0, m) = (a \cdot x_n + c) \cdot \bmod m$$

a debe ser unidad respecto a m xa que no se repitan números.

→ Comprobación de dígitos

- ISBN
  - 10 dígitos.
  - Se multiplica cada dígito por su posición (al reves, de 10 a 2).
  - Se suman.
  - Se hace el módulo 11. (Si sale 10 se pone una X)
  - Se halla el inverso.
- Tarjetas de crédito
  - Se multiplican las posiciones impares por 2 y se hace mod 9. $\Rightarrow x_k$
  - $\Sigma x_k + n + \text{DIGITOCONTROL} \equiv 0 \bmod 10$
  - n = nº de reducciones con mod 9.
- NIF
  - Número $\bmod 23 \equiv x$
  - Según x elejimos letra: TRWAGMYFPDXBNJZSQVHLCKE

→ Criptografía

- Clave simétrica (privada)
- Clave asimétrica (pública)

SIMETRICA

- Sustitución
- Por traslación
- Cifrado afin (ecuacion difántica)
- Métodos poligráficos → letra => matriz con det. ≠0

ASIMÉTRICA

- RSA.
  - Se eligen p y q primos entre sí.
  - Se halla phi(p · q) => phi(n)
  - Se halla (p·q) => n
  - Se halla $\frac{1}{h}$ mod phi(n) => e
    - → si existe inversa modular:

CLAVE PUBLICA => (h, n)
CLAVE PRIVADA => (e)

CODIFICAR := [mensaje] &^h mod n
DESCODIFICAR := [mensajecod] &^e mod n

5. COMBINATORIA

→ $|A \cup B| = |A| + |B| \underbrace{- |A \cap B|}_{\text{si son disjuntos esto es } = 0}$

→ $|A \times B| = |A| \cdot |B|$

- SIN REPETICIÓN
  - → No ordenadas

$$P(n,r) = \frac{n!}{(n-r)!} \qquad P(n) = n$$

  - → Ordenadas

$$C(n,r) = \frac{n!}{(n-r)!\,r!}$$

- CON REPETICIÓN
  - → No ordenadas

$$CR(n,r) = \binom{n+r-1}{r}$$

Con multiplicidad:

$$CR_M = \left(\frac{n!}{[\text{nº de veces que aparece cada elemento}]} \right)$$

  - → Ordenadas

$$VR(n,r) = n^r$$

6. RECORSIVIDAD

$$a_n = \underbrace{a_{n-1} \cdot C_1 + a_{n-2} \cdot C_2 + \dots + C_k \cdot a_{n-k}}_{\text{PARTE HOMOGÉNEA}} + \underbrace{g(n)}_{\text{PARTE NO HOMOGÉNEA}}$$

ejemplo:

$$a_n = \underbrace{2 \cdot a_{n-1}}_{PH} + \underbrace{1}_{PNH}$$

$a_n = r^n$

$r^n = 2 \cdot r^{n-1} = 0$

ECUACIÓN CARACTERÍSTICA ⇒ $r - 2 = 0$

$r = 2$

SOL GEN. HOM

$a_n = \alpha \cdot 2^n$

SOL. PART. NO HOMOGÉNEA

Si $\alpha = 1 \rightarrow A = 2 \cdot A + 1$; $A = -1$

$a_n = 2^n - 1$ $\qquad a_n = \alpha \cdot 2^n - 1$

Si $a_n = 1 \dots \alpha = 1 \Leftarrow$ sol. gen. h.

$$\boxed{a_n = 2^n - 1}$$

$a_n = a_{n-1} + a_{n-2}$

$a_n = r^n - r^{n-1}$

$r^n = r^{n-1} - r^{n-2}$

$r^2 - r - 1 = 0$

ECUACIÓN CARACTERÍSTICA ⇒ $r = \frac{1 \pm \sqrt{5}}{2}$

SOL. PARTS. NO HOMOGÉNEAS

$\alpha_1 = \frac{\sqrt{5}}{5}$ y $\alpha_2 = \frac{\sqrt{5}}{5}$